




UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer

Washington, D.C. 20230

February 4, 2003

MEMORANDUM FOR: Chief Information Officers

FROM: Thomas N. Pyke, Jr. 
Chief Information Officer

SUBJECT: Vulnerability Assessment Capability

We are implementing a vulnerability assessment capability to identify cyber threats and their associated vulnerabilities, and to develop mitigation strategies to those cyber threats. This vulnerability assessment capability is currently available to operating units in the HCHB to meet system Certification and Accreditation requirements and to facilitate migration to the new HCHB network. This capability is necessary to detect vulnerabilities to DOC IT infrastructure and to protect the interconnected enterprise to the maximum extent practicable. The capability will also be available to support operating units' self assessment programs, and to provide the information needed to increase overall infrastructure protection and facilitate the ability of all operating units to detect, report and share information on vulnerabilities and threats. This capability is being implemented in accordance with Presidential Decision Directive 63, Executive Orders 13231 and 13228, as well as the Federal Information Security Management Act (FISMA).

Beginning very soon, we will conduct a regular program of scheduled and "as requested" network vulnerability scans on systems located within the HCHB, beginning with the Office of the Secretary network. The scans will be limited to the identification of vulnerabilities, and will not involve actual system exploitation or compromise. Data gathered from these scans will be shared with the CIO and ITSO of the operating units involved. Please be advised that it is possible that one or more of these scans may unintentionally reach to Commerce systems and networks outside HCHB.

This new capability will soon be available for use throughout the Department, as you may request and as we work together to reduce our overall IT infrastructure vulnerability. Data collected will support the federated DOC Computer Incident Response Capability, will enhance each operating unit's ability to protect its systems from intrusion attempts, and establish system security baselines as required for such programs as patch management. This functionality will also meet the risk analysis and risk management requirements as defined within the DOC policy and FISMA.

If you have any questions, please contact Ben Chisolm at 202-482-4223 or at bchisolm@doc.gov.

cc: IT Security Officers